HOWARD COUNTY BRAC TASK FORCE
BRAC BIT: # 96
DATE: 23 September 2010
SUBJECT(S): US CYBERCOM
POINT OF CONTACT: Kent Menser (410-313-6521) kmenser@howardcountymd.gov

CyberCom Chief Details Cyberspace Defense

By Jim Garamone
American Forces Press Service

WASHINGTON, Sept. 23, 2010 - U.S. Cyber Command stands ready to defend Defense Department networks, but laws and policies must be updated to protect the nation, the organization's commander said yesterday.

Army Gen. Keith B. Alexander is the first commander of CyberCom, which stood up under U.S. Strategic Command in May, merging DOD's defensive and offensive cyber arms into one command.

The command operates in a new domain for the military – the man-made domain of cyberspace. The domain is just as important for military operations as land, sea, air and space, defense officials said. CyberCom directs military operations in cyberspace and is responsible for defense of crucial military networks.

The threat is real and continuing, Alexander said.

"The more you learn, the more you say we have to come together to protect this," the general said during a roundtable with reporters at the National Cryptologic Museum. Noting that Defense Department networks are scanned or probed 250,000 times an hour, Alexander said, "we have to do a better job defending it."

The networks are the lifeblood of commerce, power, finance and many other aspects of life today. There are 1.9 billion Internet users in the world today, Alexander said, and 4.6 billion cellular phone subscribers. The number of e-mails each day this year is around 247 billion, with 90 trillion e-mails sent in 2009. The Internet is a tremendous capability, Alexander said, but it also is an enormous vulnerability.

"Our intellectual property here is about $5 trillion," he said. "Of that, approximately $300 billion is stolen over the networks per year."

CyberCom three main missions are to defend the defense information grid, launch the full spectrum of cyber operations on command, and to stand prepared to defend the nation's freedom of action in cyberspace, Alexander said.

The command has a budget of $120 million for this year and has about 1,000 military and civilian employees. Included in this is a 24/7 joint operations center that monitors the grid, detects attacks and neutralizes them. The command works with the Air Force, Navy, Army and Marine Corps cyber commands to parcel out how to defend the networks and who has responsibility for the specific nets.

Assigning responsibility needs to happen throughout the government, the general said, noting that technology has outpaced policy and law. The government, he added, still is dealing with laws that came out when the nation relied on rotary phones.

"The laws we did 35, 40 years ago are what we have to update," he said.

Alexander put two issues on the table. "First, we can protect civil liberties and privacy and still do our mission," he said. "There can be mistakes, but we can protect the First Amendment."

The second issue, he said, is that Cyber Command is defending the DOD networks now, and as directed, can help the Homeland Security Department defend its networks.

There is confusion over who does what, the general acknowledged, so White House officials are leading an effort to sort through the needs of cybersecurity and update the policies and issues. "They are looking at the policies and authorities that need [re-]doing, and what's the right way to approach it," he said.

Once the review is finished, he explained, the president must determine how the federal government will be organized to handle this.

Congress is also looking at the problems. "From my perspective," Alexander said, "I would like to war-game it and hypothesize what could happen and ensure the policies, laws and authorities allow us to do what people expect us to do. I don't want to fail in meeting the expectations of the American people, the White House and Congress."

Changing the policy is complex, and will take time and several tries to do it right, Alexander said. The general said he envisions a team handling things in cyberspace. The DHS, the FBI, other government agencies and private stakeholders – along with CyberCom – all have a role, he said, and getting the disparate agencies and entities to work together will be a priority for cyber defense.

Some questions still need to be answered, and policy makers need to take them into consideration, Alexander said.

They include:

-- What constitutes a cyber attack?

-- How do the laws of war pertain to operations in cyberspace?

-- What does deterrence look like in the cyber world, where it can take months to determine attack perpetrators and the cyber defense group may have nothing to strike back at?

These questions are valid, the general emphasized. In 2007, Estonia was hit by a cyber attack that crippled that nation's grid for weeks, he said, and a foreign intelligence agency compromised a classified U.S. military system in 2008.

The attacks can be disruptive, like the Estonia attack, or destructive, with lives lost and equipment and networks destroyed, Alexander said.

"Those are the kind of rules that have to be weighed and discussed," he added. "It's good to have that debate, and from my perspective, it is important that it is clear who has the responsibility to defend in that kind of requirement."